

Macroscopically local correlations can violate information causality

Daniel Cavalcanti,^{1,*} Alejo Salles,² and Valerio Scarani^{1,3}

¹Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542

²Niels Bohr Institute, Blegdamsvej 17, 2100 Copenhagen, Denmark

³Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542

(Dated: December 17, 2010)

Although quantum mechanics is a very successful theory, its foundations are still a subject of intense debate. One of the main problems is the fact that quantum mechanics is based on abstract mathematical axioms, rather than on physical principles. Quantum information theory has recently provided new ideas from which one could obtain physical axioms constraining the resulting statistics one can obtain in experiments. Information causality and macroscopic locality are two principles recently proposed to solve this problem. However none of them were proven to define the set of correlations one can observe. In this paper, we present an extension of information causality and study its consequences. It is shown that the two above-mentioned principles are inequivalent: if the correlations allowed by Nature were the ones satisfying macroscopic locality, information causality would be violated. This gives more confidence in information causality as a physical principle defining the possible correlation allowed by Nature.

Introduction.— Despite quantum theory being almost one century old, its axioms remain mathematical in nature, and we are still searching for physical principles from which to derive it. After the initial discussions of the founding fathers, the operationalist viewpoint prevailed, and most were satisfied with a useful and strikingly precise theory. With the advent of quantum information science, however, a new source from which to draw principles of a more intuitive flavor was unveiled. Following this direction, many recently works have been devoted to study which tasks would be possible if correlations more general than the ones allowed by quantum mechanics could be achieved [1–7].

There are several motivations for these studies. First, they allow us to understand what is special about quantum mechanics, and consequently to get more intuition on it. Following this direction, results like the impossibility of instantaneous transmission of information [1] and of cloning, the existence of monogamy of correlation, and secrecy [2] were shown not to be particular features of quantum mechanics. Second, if one finds a practical task limiting the correlations to be quantum, this would immediately gain the status of a physically-motivated defining property of quantum correlations. In these lines, constraints on distributed computing [3], communication complexity [4] and the like, can be thought of as candidate requisites from which the theory could in principle be derived. Finally, it could be possible that quantum mechanics is not the definitive description of nature, and more general correlations might be observed in the future. Thus, some physically motivated sets of correlations which are known to be bigger than the set of quantum correlations appears as candidates for possible generalizations of quantum mechanics.

A pioneering effort in this direction was that of Popescu and Rohrlich, who asked if the impossibility of transmitting information instantaneously (*i.e.* the no-signalling principle) is enough to characterize the set of quantum correlations. It turns out that this is not the case. There exist sets of correlations satisfying the no-signalling principle that are not achievable in quantum physics. The tantamount example of this is

given by the Popescu-Rohrlich (PR) box [1].

In this vein, other information theoretic flavored principles were proposed as candidates from which the set of physically realizable correlations could be constrained [5–7]. In this work, we will be concerned with two recent proposals: Macroscopic Locality (ML) [5] and Information Causality (IC) [6]. In a nutshell, ML states that the coarse-grained statistics of correlation experiments should admit a local hidden variable model, that is, those statistics do not violate any Bell’s inequality [8]. IC, on the other hand, states that if Bob receives m bits of information from Alice, he cannot obtain more information about Alice’s system than m bits, even if he shared with her some prior resource. For the $m = 0$ case, IC simply reduces to the no-signalling principle. Formally, IC is derived by introducing a game in which Bob has to guess one of Alice’s independent and random bits (chosen at random), and bounding the sum of mutual informations of Bob’s different guesses with Alice’s actual data by the amount of one way communication from Alice to Bob.

The purpose of this work is twofold. First, we extend the IC game to the case in which Alice’s data is composed by d -dimensional alphabets (*dits*), of which Bob has to randomly guess one, allowing in principle for m dits of communication from Alice to Bob. As in the original case, we find an extremal non-signalling box that perfectly solves this task, and analyze the effect of adding noise to this set of correlations. The scenario we find in this case proves richer than the original, which allows us in turn to, second, show the inequivalence between IC and ML. In particular, we show that there exist correlations that satisfy MC, but violate IC. This implies that it is very unlikely that ML is the defining property of possibly obtainable correlations, since in this case one would have to accept that IC is violated.

We will start by reviewing the principle of ML, together with another tentative at characterizing the quantum set of correlations: the Semi Definite Program (SDP) hierarchy by Navascués, Pironio, and Acín (NPA) [9], which is intimately related with the former. We then discuss the principle of IC by

introducing our task, which generalizes the original one. We then analyze the newly found scenario and compare it to the previously known case, discussing the implications. In particular, we show how, through this extension, IC comes closer to the quantum set than ML, thus gaining more thrust as a candidate for a physical axiom defining the set of quantum correlations.

Macroscopic Locality and the NPA hierarchy.— Macroscopic Locality [5] was introduced more as a principle producing an alternative to quantum theory than as an axiom for it. Since its inception, it was known that, when considered together with the no-signalling principle, it does not give rise to the set of quantum correlations, but, instead, to a larger set. This set is precisely the one labeled by Q_1 in [9], that is, the first step in a hierarchy of SDPs that eventually converge to the quantum set. It was known already that, in some scenarios, further steps in the hierarchy are strictly contained in Q_1 , while also containing the quantum set [9]. Thus, it sufficed to prove the equivalence of Q_1 and the ML set to realize that this axiom would not suffice to fully determine quantum correlations.

ML retains its interest, though, both as an example of principle with physical content that can be put forth as candidate for axiom, and as a testable requirement from which a theory larger than quantum arises, and which could in principle be used to disprove quantum physics. As we mentioned before, it demands that classical physics be recovered in the large particle number limit by imposing that the coarse-grained correlations arising in an experiment involving a macroscopic number of particles can be modeled with local hidden variables. This requirement applied to microscopic probabilities is what gives Bell local sets of correlations, which satisfy Bell inequalities. Less restraining, ML imposes this constraint on their macroscopic counterpart; all Bell local correlations thus satisfy ML, but the converse fails to hold. To date, ML had not been contrasted with other attempts at axiomatizing quantum correlations from physical postulates.

Information Causality and its extension to arbitrary alphabet dimensions.— As we stated before, Information Causality was introduced through the use of a game with two players, Alice and Bob, and in which Alice is given N independent and random bits of which Bob has to guess one, chosen at random. In order to achieve this, they can share prior to the game any amount of physical resources they want (classical correlations, entangled states, or, in a hypothetical scenario, nonlocal post-quantum boxes), and Alice is further allowed to send m bits to Bob after she receives her input. We generalize this task by extending the alphabet in which Alice's inputs range from 2 to an arbitrary number d of dimensions. Bob then has to guess, again using prior shared resources but now allowing Alice to send him m dits, one of Alice's inputs, again chosen at random.

IC, in fact, imposes a bound on

$$I \equiv \sum_{K=0}^{N-1} I(x_K : G|y = K), \quad (1)$$

where x_K are Alice's independent and random input dits, y is Bob's random input telling him which x_K to aim for, and G is Bob's guess at that chunk of Alice's data. $I(x_K : G|y = K)$ is in turn the Shannon mutual information between Bob's guess and Alice's input x_K , given that he aims at guessing that particular input. IC, stated in general, imposes that:

$$I \leq m \log_2 d. \quad (2)$$

While all quantum correlations satisfy this requirement, it is still an open question whether there are post-quantum correlations that satisfy IC [10].

We now study to what extent the IC condition defines the quantum set. In order to do this, we consider a protocol which perfectly solves the task when an extremal set of non-signalling correlations is used as a resource. By adding noise to this box, we approach the quantum set. We start by considering the case $N = 2$. Alice and Bob share a box with d inputs on Alice's side and 2 inputs on Bob's, and d outputs on both sides (see Fig. 1). We label by a (b) the output of the box on Alice's (Bob's) side. The message Alice sends to Bob is $M = (a - x_0) \bmod d$, and Bob's guess is $G = (b - M) \bmod d = (b - a + x_0) \bmod d$.

The probability of Bob making a correct guess is:

$$\begin{aligned} P_S &= P(G = x_0, y = 0) + P(G = x_1, y = 1) = \\ &= \frac{1}{2} [P(G = x_0|y = 0) + P(G = x_1|y = 1)] = \\ &= \frac{1}{2d} \sum_{j=0}^{d-1} [P(G = x_0|x_0 = j, y = 0) + P(G = x_1|x_1 = j, y = 1)], \end{aligned} \quad (3)$$

where we used that both Alice and Bob's inputs are unbiased. In the case $y = 0$, the condition for a correct guess $G = x_0$ is equivalent to $b - a = 0 \bmod d$. When $y = 1$, we need to split the cases according to $x = j$ with $j = 0, \dots, d-1$, and the correct guess condition $G = x_j$ is equivalent, in each case, to $b - a = j \bmod d$. Putting this together, we have for the success probability:

$$\begin{aligned} P_S &= \frac{1}{2d} \sum_{j=0}^{d-1} [P(b - a = 0 \bmod d | x_0 = j, y = 0) + \\ &\quad P(b - a = j \bmod d | x_1 = j, y = 1)]. \end{aligned} \quad (4)$$

Consider now the case in which Alice and Bob share a box defined as:

$$\text{PR}_0(ab|xy) \equiv \begin{cases} 1/d & \text{if } x \cdot y = (b - a) \bmod d \\ 0 & \text{otherwise} \end{cases}, \quad (5)$$

with $a, b, x \in \{0, \dots, d-1\}$, and $y \in \{0, 1\}$. This is a straightforward generalization of the PR box [1], to which

it reduces in the case $d = 2$. It is extremal in the $d2dd$ non-signalling polytope, as can be verified by using the same counting argument as in the proof of Theorem 1 of Ref. [12]. This box clearly satisfies $P(b - a = x.y \bmod d | xy) = 1$, which leads to a probability of success equal to unity (which is the case depicted in Fig. 1). This in turn implies $I = 2 \log_2 d$, which violates the IC condition (2) since $m = 1$.

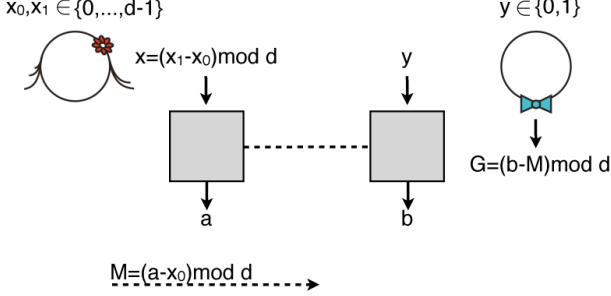


FIG. 1: **Information Causality protocol for d -dimensional alphabets.** Suppose Alice is given two dits, x_0 and x_1 , while Bob gets a bit y . Bob is asked to guess the value of one of Alice's dits, according to the value of y . In the case that Alice and Bob share the noiseless box (5) they can solve this problem perfectly. In order to do that Alice inputs $(x_1 - x_0) \bmod d$ into the box, while Bob inputs y . After receiving her output a , Alice sends a message $M = (a - x_0) \bmod d$, corresponding to one dit of communication. Bob, in possession of M , makes his guess $G = (b - M) \bmod d = (b - a + x_0) \bmod d$. Given that the box behaves as $x.y = (b - a) \bmod d$, Bob computes the value $G = [(x_1 - x_0).y + x_0] \bmod d$, which equals x_0 if $y = 0$ and x_1 if $y = 1$.

We now define an isotropic noisy box as follows:

$$\begin{aligned} \text{PR}(E) &\equiv E \text{PR}_0 + (1 - E) \mathbb{1} \\ &= E \text{PR}_0 + \frac{1 - E}{d} (\text{PR}_0 + \dots + \text{PR}_{d-1}), \end{aligned} \quad (6)$$

that is, a mixture of the generalized PR box (5) and a box $\mathbb{1}$, representing classical random noise. Box $\mathbb{1}$ outputs completely random dits regardless the inputs, and can be decomposed, as we did in the second line of Eq. (6), in terms of PR_0 plus $d - 1$ other extremal non-signalling boxes, denoted by PR_j with $j \in \{1, \dots, d - 1\}$, s.t.

$$\text{PR}_j(ab|xy) \equiv \begin{cases} 1/d & \text{if } x.y = (b - a) + j \bmod d \\ 0 & \text{otherwise} \end{cases}. \quad (7)$$

The parameter E ($0 \leq E \leq 1$) quantifies the amount of noise in the box. This noisy correlations satisfy $P(B - A = x.y \bmod d | xy) = \frac{(d-1)E+1}{d}$ so we have for the success probability $P_S = \frac{(d-1)E+1}{d}$.

Although we could search for the critical value of E for a single box to stop violating IC, it was seen already in the original $d = 2$ case that this is not optimal [6]. Instead, one needs to consider the task illustrated in Fig. 1 for an arbitrary input size N , and extend the protocol described by nesting many instances of it.

For the case of isotropic noisy boxes and $d = 2$, it was seen that a suitable nesting of the protocol was enough to recover the quantum bound [6]. In the Appendix, we describe this nesting and its extension to arbitrary dimension d . This extension proves straightforward, apart from the consideration of the cancellation of errors of different boxes, which now happens less frequently due to the larger outcome alphabet. We find a recurrence relation for the probability of success, and by solving it, we get for the success probability of n boxes (see the Appendix for details):

$$P_S^{(n)} = \frac{(d-1)E^n + 1}{d}. \quad (8)$$

This is the probability of Bob producing a correct guess after the use of n boxes. Note that, given the structure of the nesting, one needs to use $n = \log_2 N$ boxes if the input consists of N dits.

In order to study the violation of IC in terms of the probability of a successful guess, we use Fano's inequality [11] to bound I , as was already discussed for arbitrary d -dimensional alphabets in [6]:

$$I \geq 2^n (\log_2 d - h(P_S) - (1 - P_S) \log_2(d - 1)), \quad (9)$$

where $h(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$ is the binary entropy, and we set equal probabilities for the correct guessing of the different dits, as is the case in the protocol. Considering then this bound for the success probability in the nested protocol given in Eq. (8), we obtain:

$$I \geq 2^n \left[\log_2 d - h\left(\frac{1 + (d-1)E^n}{d}\right) + \frac{d-1}{d} (1 - E^n) \log_2(d - 1) \right]. \quad (10)$$

Consequences of the IC extension and inequivalence with ML.— We now turn to the consequences of the extension of IC we have introduced. In Fig. 2 we show the critical value of E for which IC ceases to be violated, as a function of the number of boxes used, n , and for different values of d . This value is obtained from (10). For $d = 2$, the critical value of E asymptotically approaches Tsirelson's bound $E_T = 1/\sqrt{2} \simeq 0.707$, which defines the extent of the quantum set for isotropic correlations. Therefore, we recover the result that IC defines isotropic quantum correlations for $d = 2$, which also coincide with those satisfying ML (or, equivalently, are in Q_1). It was shown, however, that this protocol does not define the entire quantum boundary even for $d = 2$ [10].

For larger values of d , however, the situation proves richer. First, we notice that for sufficiently large d , the curves go below the critical value E_T . This value is therefore no longer representative of the extent of quantum correlations. However, it still defines the extent of Macroscopically Local isotropic correlations, as we have checked for values of d up to 5 by solving the SDP that defines the set Q_1 . This thus proves the

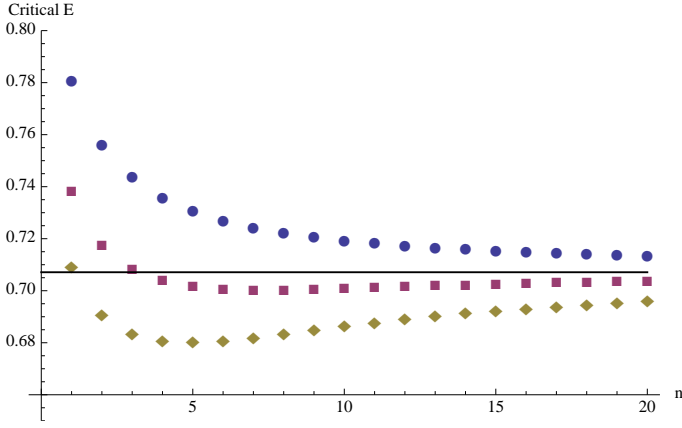


FIG. 2: **Critical noise level for IC violation.** We plot the critical amount of noise for which IC ceases to be violated, as a function of n , and for different values of d ($d = 2$ circles, $d = 5$ squares, $d = 10$ diamonds). The solid line corresponds to $1/\sqrt{2}$, which, according to our numerical calculations up to $d = 5$, coincides with ML.

d	E_{IC}	E_{ML}	E_Q
2	0.707	0.707	0.707
3	$\lesssim 0.708$	0.707	?
4	$\lesssim 0.705$	0.707	?
5	$\lesssim 0.700$	0.707	?

TABLE I: **Critical values of noise for increasing alphabet dimension.** Here, E_{IC} is the critical noise for which IC ceases to be violated using the protocol described, optimized over n . E_{ML} is the corresponding value for ML correlations (Q_1), and E_Q is the extent of the quantum set, ignored apart from the $d = 2$ case. All values to 10^{-3} accuracy.

inequivalence of ML and IC. Table I summarizes the critical values obtained for the different sets.

Unfortunately, using either numerical searches or plausible analytical guesses, we were unable to find quantum realizations for the isotropic correlations defined by E_{IC} for $d > 2$ above the local boundary. So, contrary to the $d = 2$ case, we do not know if the IC strategy studied here reaches the quantum boundary. We sketch the situation pictorially in Fig. 3, where we compare the $d = 2$ and larger d cases.

Finally, we stress a curious feature of the curves presented in Fig. 2. Differently from the $d = 2$ case, in which the critical level of noise monotonously approaches E_T , for larger values of d the curves display a minimum in the critical noise for a finite value of n . The position of this minimum further decreases with increasing d . While this effect is not yet fully understood, it might hint towards the non-optimality of the protocol considered. We leave this question for further investigations.

Discussion.— We have extended the principle of IC to arbitrary input alphabet dimensions and studied the consequences of this extension. The scenario we found turned out to be richer than the original case, even if only considering isotropic

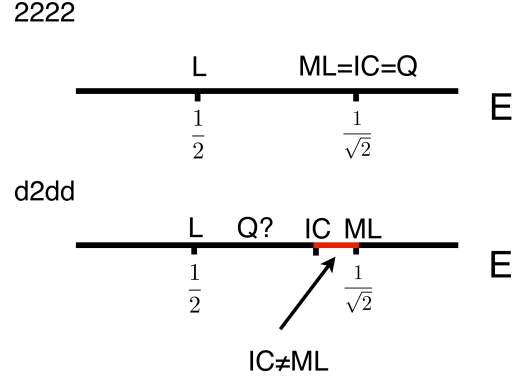


FIG. 3: **Scenario comparison for the 2222 and $d2dd$ cases.** In the 2222 case both IC and ML stop being violated for the same amount of noise $E = 1/\sqrt{2}$. For the case $d2dd$ with $d > 2$, the violation of IC can stand more noise than that of ML, which shows that ML correlations can violate IC.

correlations. This allowed us to show the inequivalence between IC and ML. The extension we presented might prove useful in deciding whether IC is a good candidate as axiom for quantum correlations, question that still remains open.

As a final remark, we note that the extension remains valid in the $d \rightarrow \infty$ case. Interestingly, through this extension, Bob would be able to guess (to arbitrary precision) either one of two arbitrary precision floating point numbers of Alice using just one of the extremal $d2dd$ boxes we introduced. How this compares as a resource to an asymptotic number of standard PR 2222 boxes is a question for further study.

Acknowledgements.— We would like to thank Tomasz Paterek, Nicolas Brunner, Andreas Winter and Michael Wolf for discussions. We acknowledge financial support by the EU STREP COQUIT under FET-Open grant number 2333747, National Research Foundation and the Ministry of Education of Singapore.

* Electronic address: dcavalcanti@edu.nus.sg

- [1] S. Popescu, D. Rohrlich, Found. Phys. **24**, 1379 (1994).
- [2] L. Masanes, A. Acín, and N. Gisin, Phys. Rev. A. **73**, 012112 (2006).
- [3] N. Linden, S. Popescu, A. J. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
- [4] W. van Dam, arXiv quant-ph/0501159 (2005). G. Brassard, *et al.*, Phys. Rev. Lett. **96**, 250401 (2006).
- [5] M. Navascués and H. Wunderlich, Proc. Roy. Soc. Lond. A **466**, 881-890 (2009).
- [6] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Żukowski, Nature **461**, 1101-1104 (2009).
- [7] J. Oppenheim, S. Wehner, arXiv:1004.2507v1.
- [8] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
- [9] M. Navascués, S. Pironio, A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); New J. Phys. **10**, 073013 (2008).

- [10] J. Allcock, N. Brunner, M. Pawłowski, V. Scarani, Phys. Rev. A **80**, 040103 (2009).
- [11] M. Nielsen, I. Chuang, *Quantum Information and Computation* (Cambridge University Press, Cambridge, UK, 2001).
- [12] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, Phys. Rev. A **71**, 022101 (2005).

APPENDIX: NESTED PROTOCOL

Here we discuss the nesting of the protocol described in the main text needed in order to tackle the task when $N > 2$. The nesting process is similar to that originally presented in [6], but differs in the treatment of accumulated errors. For clarity, suppose Alice is given $N = 4$ dits, x_0, x_1, x_2 , and x_3 , of which Bob has to learn one, indexed by the random bits he receives, y_0 and y_1 (see Fig. 4). Now Alice and Bob share three boxes. If these were the noiseless PR_0 boxes of Eq. (5), they could perfectly solve the task. The main idea (explained in details in Fig. 4) is that they can use the first box to reveal the value of either x_0 or x_1 , the second box to x_2 or x_3 . In the first case Bob would have to know a message M' , while in the second M'' . Since only one message can be transmitted, they use the third box to reveal to Bob either M' or M'' , depending on which dit he wants to know.

Clearly, this process can be repeated an arbitrary amount of

times, with Alice and Bob sharing $2^n - 1$ boxes for a task involving $N = 2^n$ dits. Note however that only n of these boxes are actively used in the protocol, in the sense that the outcome of the remaining ones is irrelevant for the correctness of the guess. So now we look at how the errors accumulate in the different stages of the nested protocol. The joint probability of success for two different boxes α and β is given by:

$$P_S^{\alpha\beta} = P_S^\alpha P_S^\beta + \frac{1}{d-1}(1 - P_S^\alpha)(1 - P_S^\beta), \quad (11)$$

where the first term corresponds to both boxes succeeding, and the second term arises from error compensation: of the $(d-1)^2$ “ α wrong, β wrong” events, only $d-1$ lead to a cancellation. We can now think of the probability of success for $n+1$ boxes as the joint success of n boxes and a single box:

$$P_S^{(n+1)} = P_S^{(n)} P_S + \frac{1}{d-1}(1 - P_S^{(n)})(1 - P_S). \quad (12)$$

This recurrence can be solved for $P_S = \frac{(d-1)E+1}{d}$, the probability of success of a noisy PR box, to finally get:

$$P_S^{(n)} = \frac{(d-1)E^n + 1}{d}. \quad (13)$$

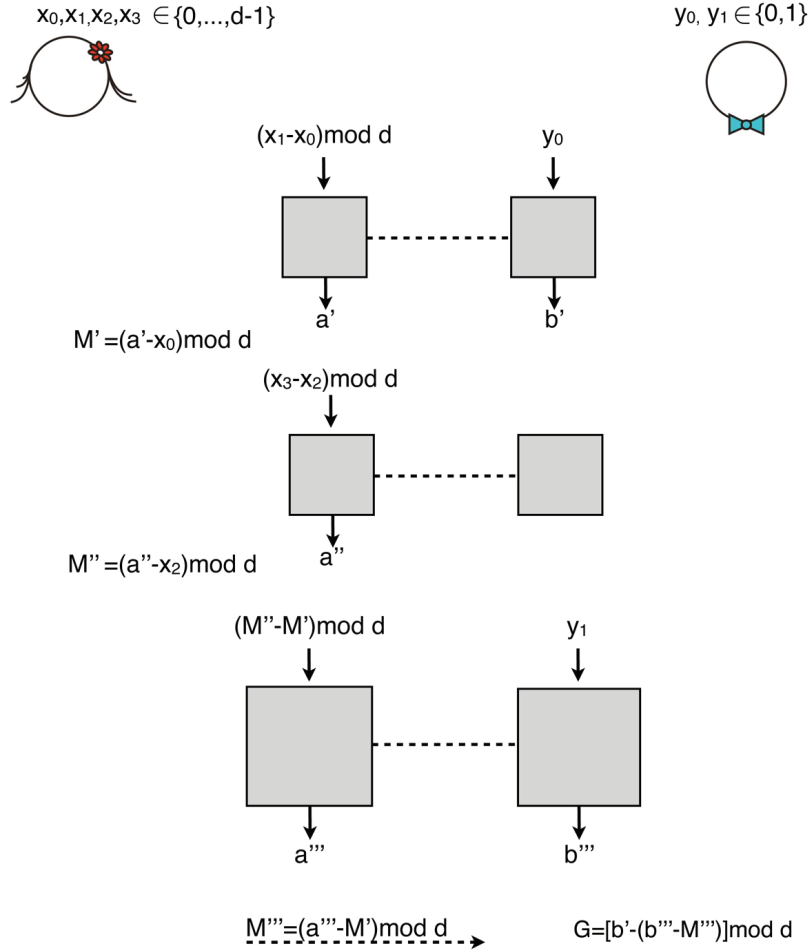


FIG. 4: **Nesting of the protocol for $N > 2$.** We illustrate how to recursively employ the $N = 2$ protocol in order to solve the IC task for larger values of N . Depicted is the case of $N = 4$, where Bob aims to know the value of either of the four dits x_0, x_1, x_2 , or x_3 . Alice inputs $(x_1 - x_0) \bmod d$ in the first box, and would have to send the message $M' = (a' - x_0) \bmod d$ to make Bob to be able to know either x_0 or x_1 . She proceeds similarly in the second box, but now using x_2 and x_3 . In this case the message she would send would be $M'' = (a'' - x_2) \bmod d$. Since she can send only one message, they use a third box to make Bob able to know either M' or M'' . To this end, Alice inputs $(M'' - M') \bmod d$ to the third box, and sends the message $M''' = (M'' - M') \bmod d$ to Bob. By inputting $y_1 = 0, 1$ to the third Box he can guess the value of M' or M'' , depending on which dit he is looking for. Having this information he uses either box 1 or box 2 to discover the dit he aims for. In the figure we supposed that Bob wants to know the value of either x_0 or x_1 . In this case he would input $y_1 = 0$ in the third box, find the value of M' , input y_0 to first box and finally guess the value of the bit he wants according to $G = [b' - (b''' - M''')] \bmod d$. For arbitrary N this process can be iterated straightforwardly.